Call for Public Input on Proposed Elections ICT Regulations

The Elections Laws (Amendment) act 2016 came into force on 4th October 2016. This legal amendment requires the Commission to develop a policy on the progressive use of technology in the electoral process and also make regulations for the adoption and implementation of technology in the electoral process. The Act further establishes an integrated electronic electoral system consisting of voter registration, voter identification and results transmission that shall be used in the next general election.

The commission has already deployed several technologies that play significant role in the delivery of the commissions mandate, vision and mission. A clear ICT policy framework that allows the commission to progressively adopt ICTs in the electoral process has been drafted to govern the deployment of technologies in the Electoral process.

The Commission in line with the amended Act has established an Elections Technical Advisory Committee to oversee the adoption of technology. The Committee is composed of technical industry players and other stakeholders. Its first meeting was held on Wednesday 26 October2016.

In line with the principle of public participation, the Commission is welcoming contributions on the proposed draft regulations on or before 31st October, 2106.

Comments can be sent on email to: ictregulations@iebc.or.ke

A. PROPOSED REGULATIONS

Title: *Elections (Information and Communication Technology) Regulation, 2016*

Thematic Area	ICT Draft Policy	Proposed Regulations	Comments
Transparent acquisition and disposal of ICT assets and systems Electoral Act, S. 44 (5) (a) (Amendment)	"The commission shall establish and maintain a framework to manage IT-enabled investment programs that encompasses cost, benefits, prioritization within budget, a formal budgeting process and management against the budget. The commission shall acquire and dispose of the electoral systems in line with the PPDA and PFMA. " **a) Identification of electoral systems** "The need for a new application/function or infrastructure for use in electoral process shall be analyzed before acquisition in order to translate business functional and control requirements into an effective	*1. The Commission will conduct a system needs assessment and determine whether there is a requirement to upgrade the existing system, or acquire new systems.* *2. The Commission shall develop requirements for new systems, and shall consult with stakeholders.* *The Commission shall procure the technology in accordance with the Public Procurement and Asset Disposal Act (PPAD) and other relevant laws and regulations.*	This policy is included in the first paragraph -before the acquisition/ procurement.

Thematic Area	ICT Draft Policy	Proposed Regulations	Comments
	and efficient design of automated solutions by identifying technically feasible and cost effective solutions"		
	b) Acquire and Maintain Technology Infrastructure "The commission shall acquire and maintain an integrated and standardized ICT infrastructure through provision of appropriate platforms for the business applications in line with the defined ICT architecture and technology standards"	*3. The Commission shall ensure proper maintenance of ICT systems to guarantee serviceability, reliability and availability.*	This policy is reflected in the second paragraph on procurement.
	a) Disposal, Servicing and Transfer of IT Equipment Policy "Whenever the commission relinquishes *custody* of IT equipment or its components, whether to lend, *donate*, service or dispose of the equipment, the commission shall take reasonable measures to prevent the unauthorized release of information. The commission shall implement policies and associated procedures in compliance with the Public Procurement and Disposal Act and shall ensure that employees,	*4. The Commission shall comply with the PPAD and its applicable regulations during the disposal of ICT assets.* *5. After conducting an assessment, the Commission will determine whether to dispose or retain.*	Check the ICT Act.

Thematic Area	ICT Draft Policy	Proposed Regulations	Comments
	contractors, temporary personnel and other agents of the commission adhere to those policies.		
Testing and certification of the system Electoral Act, S. 44 (5) (b) (Amendment)	"ICT shall install and accredit electoral systems to ensure that new or changed systems are working properly by testing the applications and infrastructure solutions to ensure that they are fit for the intended purpose and are free from errors and planning releases to production, the commission shall authorize the all electoral systems prior to formal use"	*6. The Commission shall ensure timely end-to-end testing of electoral technologies before deployment for the election and address any challenges as necessary.* *The Commission will define the period of testing in geographical areas and will publish this information before the testing takes place.* *The Commission will issue a public notice specifying the date, time and place of the testing to invite stakeholders to attend. The Commission may publish this information on its official website, in the media outlets, or posted outside of the Commission's office.* *7. After the Commission conducts the necessary testing of electoral technologies, a certification report shall be prepared by the Commission. The Commission may request a certification by an independent body.*	Use consistent wording: electoral technology was chosen as a more general term (instead of electoral systems or integrated electoral systems). Note: It is only an invitation for stakeholders to attend. If stakeholders are not present, the testing will proceed.
Mechanisms for the conduct of a system audit	"The commission shall continually assess potential risks and vulnerabilities to the electoral systems	*8. The Commission shall continuously audit the electoral technologies to ensure that it meets the functional and non-functional requirements.*	

Thematic Area	ICT Draft Policy	Proposed Regulations	Comments
Electoral Act, S. 44 (5) (c) (Amendment)	and develop, implement, and maintain appropriate administrative, physical, and technical security measures for purposes of mitigating the identified information security risks. Audit trails shall be maintained to provide accountability for the use of information resources within the commission" "The commission shall monitor and evaluate internal information security process controls to ensure compliance with international best practice(ISO/IEC 27001:2013 Standard) and IT-related laws and regulations through monitoring the internal control processes for IT-related activities and identifying improvement actions"	*The Commission will conduct audits of the electoral technologies regularly or as may be required. The Commission may conduct audit internally, or may decide to contract a professional firm.* *The Commission will issue procedures to further define the audit process.* *9. For the purpose of auditing the Registers of Voters, section 8 (A) of the Electoral Act defines the process and timeline for the conduct of the audit.*	Discussion on standards for audit: could be further defined in a procedure or guideline.
Data storage and information security	"ICT shall manage and ensure optimal use of the electoral data by ensuring that that information is available as	*10. The Commission shall put in place mechanisms to ensure data availability, accuracy, integrity, and confidentiality.*	The Commission will follow asset disposal rules.

Thematic Area	ICT Draft Policy	Proposed Regulations	Comments
Electoral Act, S. 44 (5) (d) (Amendment)	required, maintaining the completeness, accuracy and protection of data" "ICT shall ensure systems security by maintaining the integrity of information and processing infrastructure and minimizing the impact of security vulnerabilities and incidents by defining ICT security policies, procedures and standards, and monitoring, detecting, reporting and resolving security vulnerabilities and incidents" **a) Data Classification Labels:** "To help ensure that all sensitive electoral information is protected, the commission shall classify data, systems, media, devices and electronic transmissions" **b) Classification Methodology:** The commission shall systematically go through a data classification process and shall document their classification decisions.	*11. The Commission will adopt monitoring tools to prevent, detect and mitigate vulnerabilities in the ICT infrastructures and breaches of security.* *12. The Commission shall classify data to determine the level of accessibility in line with the Access to Information Act.* *13. A person may present a formal request to the Commission to acquire information in accordance with existing General Election Regulations or other laws.*	This provision addresses policy on security and potential failure of technology. Check exact provision of Access to Information Act. Check provisions of General Election Regulations regarding request for information and disclosure.

Thematic Area	ICT Draft Policy	Proposed Regulations	Comments
	c) Secure Sensitive Data at Rest: "The commission shall secure sensitive data at rest. Regardless of whether access is via trusted or untrusted channels, the commission shall provide strong access controls for sensitive data at rest. As a minimum, the commission shall protect sensitive data at rest through encryption." **d) Secure Backups:** "The commission shall apply encryption consistently to backup devices, media and active data for sensitive data backups and restorations. Data backups should enforce the most current access controls." **e) Secure Sensitive Data on Portable Devices and Media:** "As a minimum, the commission shall implement controls for the placement of sensitive data on portable devices and media: The commission shall authorize the placement of sensitive data onto portable devices and media."		The draft policy is very detailed. All these following provisions do not need to be included in the draft regulations. Guidelines and procedures could be issued to further defined those processes.

Thematic Area	ICT Draft Policy	Proposed Regulations	Comments
	f) Physically Secure Sensitive Data: The commission shall secure the physical devices, locations and facilities used for sensitive data processing and storage.		
	g) Communicate Expectations for Handling Sensitive Data: The commission shall ensure that the public is aware of all of the requirements associated with the protection of sensitive data and that they actively acknowledge their role.		
	h) Be Prepared to Respond to a Potential Breach: The commission shall develop incident response procedures that specifically address a compromise of the security of sensitive data.		This is addressed in the section above about vulnerabilities and below section.
	i) Secure Sensitive Data in Transmission: The commission shall secure sensitive data in transmission. Whenever sensitive data travels over the Internet or other untrusted channels, as a minimum, encryption shall be used to safeguard the data. The commission		

Thematic Area	ICT Draft Policy	Proposed Regulations	Comments
	shall ensure that a cryptographic key management plan is in place that protects the creation, distribution and storage of cryptographic keys.		
Data retention and disposal Electoral Act, S. 44 (5) (e) (Amendment)	"The commission shall maintain and retain enterprise information and records in compliance with applicable governmental and regulatory requirements. The commission will adhere to retention schedules and destruction procedures in compliance with regulatory, business, and legal requirements. The commission shall endeavor to comply with the Public Procurement and Disposal Act, "Disposal, Servicing and Transfer of IT Equipment,"	*14. The Commission will issue a procedure on data retention and archiving in accordance with the Commission's existing laws and regulations.*	Discuss the potential issuance of procedures. See, Ongoing Record and Archiving Management. See, Public archive and documentation service act.
Access to electoral system software source codes Electoral Act, S. 44 (5) (f) (Amendment)	"The commission shall enter into escrow agreements with the electoral system software vendors to ensure secure access to system source codes"	*15. The Commission shall ensure secure access to system source codes with software vendors and shall clearly define the terms of access to source codes.* *16. The Commission may allow access to the source code in accordance with its policy/procedures/guidelines.*	Clarify interpretation of "access source code" by parliament. Example: in case of a court order during election dispute

Thematic Area	ICT Draft Policy	Proposed Regulations	Comments
Capacity building of staff of the Commission and relevant stakeholders on the use of technology in the electoral process. Electoral Act, S. 44 (5) (g) (Amendment)	"The commission shall acquire, maintain and motivate a competent IT workforce for creation and delivery of IT services to the commission and the public" "IT processes shall be agile in responding to the business strategy while complying with governance requirements and providing defined and competent points of contact by focusing on establishing transparent, flexible and responsive IT organizational structures and defining and implementing IT processes with owners, roles and responsibilities integrated into business and decision processes" "ICT shall enable operation and use of technology by ensuring satisfaction of end users with service offerings and service levels, and seamlessly integrating applications and technology solutions into business processes by providing effective user	*17. The Commission shall implement a continuous and comprehensive training (or capacity building) programs for its internal staff and conduct training for stakeholders within sufficient time before election day.* *18. The trainings on technology shall include a detailed and comprehensive curriculum approved by the Commission.* *19. The Commission shall ensure that technical curriculum includes both practical (hand-on) training as well as theoretical aspects for a sufficient time approved by the Commission.* *a) Such practical and technical training shall be conducted by* *a. Qualified personnel with adequate knowledge and experience on the subject matter, and* *b. Service providers of such technology shall be required to ensure adequate knowledge and skills transfer to the Commission staff to be able to maintain and operate the technologies.*	Development of training manual and procedures. For Capacity building, it is important to take into consideration resources available and HR policy and plan. Distinguish between internal and external training. Suggestion to train a pool of trainer on technology.

Thematic Area	ICT Draft Policy	Proposed Regulations	Comments
	and operational manuals and training materials to transfer the knowledge necessary for successful system operation and use." "ICT shall define and manage service levels ensuring the alignment of key ICT services with business strategy by focusing on identifying service requirements, agreeing on service levels and monitoring the achievement of service levels." "ICT shall manage performance and capacity to ensure optimal performance of ICT infrastructure, resources and capabilities in response to business needs, meeting response time requirements of service level agreements, minimizing down time and making continuous ICT performance and capacity improvements through monitoring and measurement" "ICT shall educate and train users to provide for effective and efficient use of electoral technology solutions and	*b) The Commission shall ensure that the service providers shall provide sufficient training on both the technical and operational aspects of the System.* c) *The Commission shall ensure that adequate and continuous support agreements with service providers are established for effective and sustainable use of technologies.*	

Thematic Area	ICT Draft Policy	Proposed Regulations	Comments
	user compliance with policies and procedures."		
Telecommunication network for voter validation and result transmission Electoral Act, S. 44 (5) (h) (Amendment)	"The commission shall secure sensitive data in transmission. Whenever sensitive data travels over the Internet or other untrusted channels, as a minimum, encryption shall be used to safeguard the data. The commission shall ensure that a cryptographic key management plan is in place that protects the creation, distribution and storage of cryptographic keys"	*20. The Commission will disclose any engagement with telecommunication service providers that may have prior contractual engagements with political entities.* *21. Telecommunication network service providers shall be obliged to provide and deliver services as may be requested by the Commission.* *22. The Commission shall identify and communicate in a timely manner to all stakeholders the network service available at different polling stations and where no network service is available, the Commission shall inform the stakeholders and publish this information.* *23. In areas where there is no available telecommunication network, the Commission will put in place alternative mechanisms for transmission.* *24. The Commission shall establish appropriate infrastructure for voter validation.* *25. The Telecommunication network service*	Purpose is to avoid conflict of interest. Transparency. Basic requirements for the network could be set in procedure or guideline, so that every service provider will have to meet. Geographical diversity of environment should be taken into consideration. There is a need for contingency plan in case failure or weak network – never 100% guarantee. Environment changes on election day.

Thematic Area	ICT Draft Policy	Proposed Regulations	Comments
		providers shall ensure security, traceability and availability of the network during the entire election period, or during other period as may be required by the Commission.	
Development, Publication and Implementation of a disaster recovery and operations continuity plan Electoral Act, S. 44 (5) (i) (Amendment)	"ICT shall ensure continuous service by ensuring minimum business impact in the event of an ICT service interruption through building resilience into the electoral technology solutions and developing, maintaining and testing ICT continuity plans"	*26. The Commission shall establish a business continuity plan detailing both operational and technical processes, procedures and tools.* *27. The Commission shall test the business continuity plan to ensure that all operational procedures are working as intended.* *28. The Commission shall maintain a disaster recover site for all electoral information systems.* *29. The Commission will establish such data recovery processes, procedures and tools, as may be necessary to ensure quick and efficient data recovery in the event of technology malfunctions.* *30. The Commission shall maintain such physical documentation records of the voters to enable re-construction of the information in the event of data loss during transmission.* *31. The commission shall ensure that such other failover technologies, and/or procedures exist to ensure business continuity.*	Importance of building resilience. In case of interruption, ensure minimum impact. + Guarantee lesser impact in case of failure. + Measures to prevent potential attacks.

Thematic Area	ICT Draft Policy	Proposed Regulations	Comments
		32. The Commission shall ensure that the provisional results transmitted electronically are validated and verified to eliminate any transcription errors and reconcile with the physical official results forms.	
Operations of the Elections technical Advisory Committee (ETAC) Electoral Act, S. 44 (5) (j) (Amendment)		*33. Mandate: In accordance with its constitutional mandate to conduct and supervise elections, the Commission will take decisions on electoral technology. As provided in Article 44 of Electoral Act, the Commission will establish an Election Technical Advisory Committee (ETAC) to provide comments or formulate advice on electoral technology for the Commission's consideration and approval.* *34. Role and responsibilities: The ETAC will provide advice on the Adoption and Implementation of electoral technology in the Commission, in particular* *a) the Biometric voter registration, biometric voter identification and results transmission systems and such other electoral systems.* *b) The development of policies for the progressive use of technology in the electoral process.* *c) Timely acquisition of such technology*	Clarify that the role of ETAC is advisory, and the Commission remain the decision making power. Comment: allowances for

Thematic Area	ICT Draft Policy	Proposed Regulations	Comments
		necessary for the conduct of an election *d) Ensure open and transparent testing, verification and deployment of electoral technology.* *e) Coordinate participation of stakeholders in the implementation and deployment of electoral technology.* *f) To regularly engage with stakeholders in order to sensitize them on the progress of adoption and use of technology in the electoral process,* *g) Receive regular updates from key service providers on their readiness to support the electoral process.* *35. Composition: The ETAC will be composed of members and staff of the Information and Communication Technology (ICT) Committee of the Commission, and representatives of the following institutions:* *a) Two members representing the political parties' liaison committee.* *b) One representative from the Commission on Administrative Justice* *c) One representative from the Principal Secretary, National treasury,* *d) One representative from the Principal Secretary, Ministry of ICT,*	Commission and staff should be clarified.

Thematic Area	ICT Draft Policy	Proposed Regulations	Comments
		e) One representative from the The registrar of political parties. *f) One representative from the Director General of Communication Authority of Kenya,* *g) One representative from the Kenya Private Sector Alliance.* *h) One representative from the Technology service providers association (TESPOK)* *i) One representative from the Information Systems Audit and Control Association (ISACA)- Kenya Chapter.* *j) One representative from the Attorney General Office,* *k) One representative from the National Registration Bureau, and* *l) And any other body as may be deem necessary by the Commission.* *36. Each institution shall appoint a representative to attend the meetings of ETAC at the level of PS, CEO or Director level.* *37. The Commission shall chair and provide secretariat services to the committee. The Commission will be responsible for convening meetings of ETAC.*	

Thematic Area	ICT Draft Policy	Proposed Regulations	Comments
		38. Meetings of ETAC shall be held at least twice a year, and as deemed necessary by the Commision . *39. The Commission shall provide sitting allowances for the members, but will not provide any salary, or any other benefits.* *40. Report: The Commission will publish regular information on the meetings held by ETAC.* *41. The Commission will issue guidelines/TOR to further define the functions, modalities and methods of work of the ETAC.*	
IT Risks Assessment and Management	"A risk management framework that is integrated in business and operational risk management frameworks, risk assessment, risk mitigation and communication of residual risk shall be created and maintained. Risk mitigation strategies shall be adopted to minimize residual risk to an accepted level. The result of the assessment shall be expressed in financial terms, to enable stakeholders to align risk to an acceptable level of		

Thematic Area	ICT Draft Policy	Proposed Regulations	Comments
	tolerance. It shall involve analyzing and communicating IT risks and their potential impact on business processes and goals"		
Change Management	"ICT shall manage changes to respond to business requirements in alignment with the business strategy, whilst reducing solution and service delivery defects and rework through impact assessment, authorization and implementation of all changes to the ICT infrastructure, applications and technical solutions, minimizing errors due to incomplete request specifications and halting implementation of unauthorized changes"		

Thematic Area	ICT Draft Policy	Proposed Regulations	Comments
Third-party Services Management	"ICT shall manage third-party services providing satisfactory third-party services while being transparent about benefits, costs and risks establishing relationships and bilateral responsibilities with qualified third-party service providers and monitoring the service delivery to verify and ensure adherence to agreements"		
Regulatory Compliance Management	"The commission shall ensure regulatory compliance with laws and regulations by identifying all applicable laws and regulations and the corresponding level of IT compliance and optimizing IT processes to reduce the risk of non-compliance"		